ABSTRACT

The present invention provides new ways to securely backup and restore a user's portable biometrics-based authentication device without compromising the secrecy thereof. A two-tier backup encryption structure allows the decryption of lower tier data only when upper tier data has been decrypted and validated. The structure can be expressed as:

Backup ={biometrics data + any validation scripts/keys/values + (associated data)}, where

( ) represents the lower tier encryption; and

{ } represents the upper tier encryption.

The lower tier data contain encrypted electronic identity of a user and authentication information associated therewith such as private keys and corresponding certificates. The upper tier data contain the encrypted lower tier data and the user's biometrics information.